监控EIGRP在连结7000上的邻接变化的SNMP陷阱

Contents

Introduction

本文描述简单网络管理协议(SNMP)陷阱监控增强的内部网关路由选择协议(EIGRP)在连结7000上的邻接变化。连结只支持EIGRP-MIB的两个陷井， cEigrpAuthFailureEvent和cEigrpRouteStuckInActive，但是up/down EIGRP的相邻的没有SNMP陷阱(cEigrpNbrDownEvent)。

形成SNMP陷阱的一个可行的解决方法监控EIGRP邻接更改是配置-一个相邻的和一个下来相邻的-被触发的两个EEM脚本基于Syslog模式。

示例

```
event manager applet EIGRP_TRAP_nbr_dwn
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*down"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Down"
event manager applet EIGRP_TRAP_nbr_up
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*up"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Up"
```

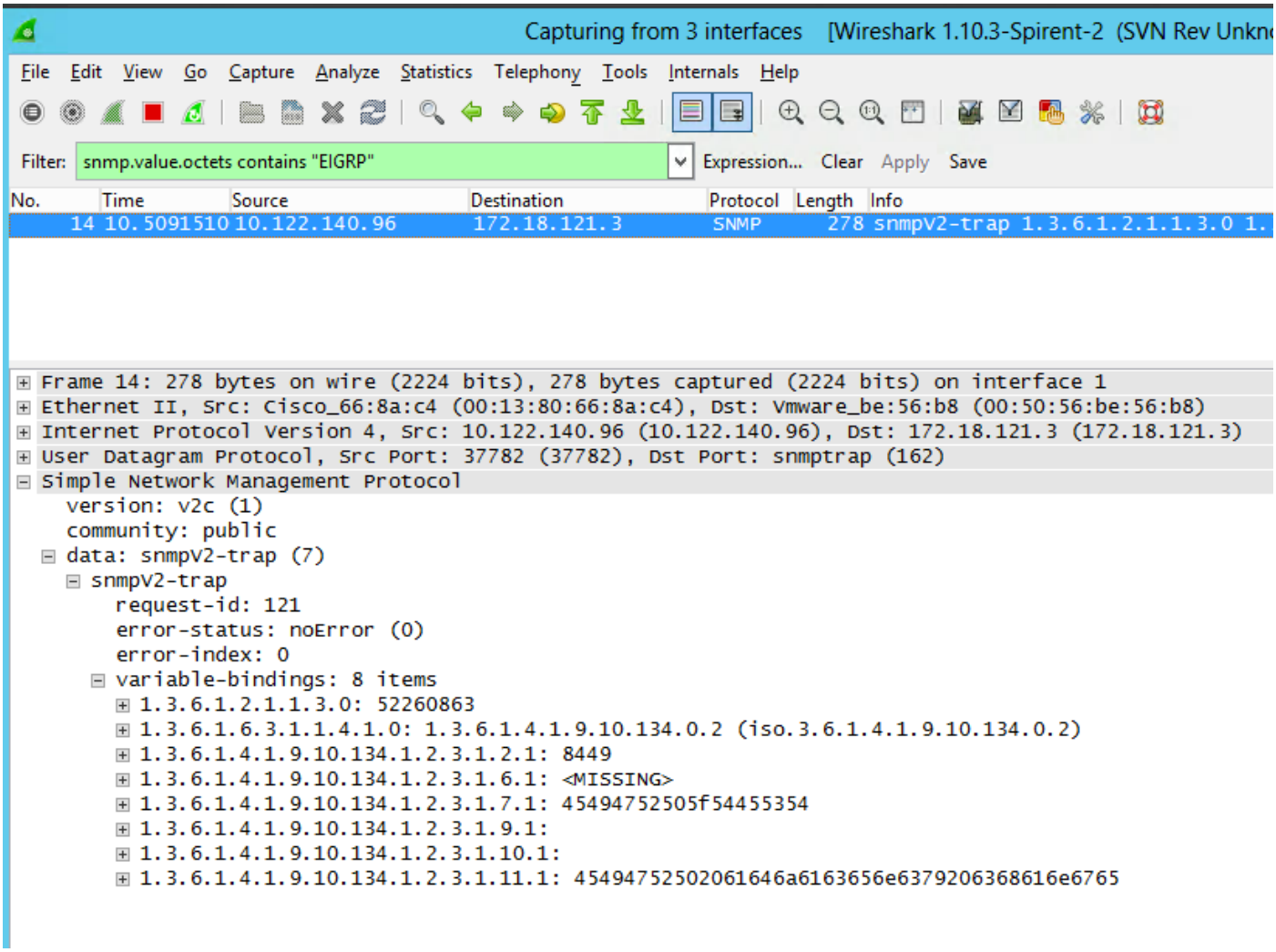
您能通过拍动然后测试第3层接口(您能创建测试交换机 虚拟接口(SVI)验证至于不打乱连接) ：

```
event manager applet EIGRP_TRAP_nbr_dwn
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*down"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Down"
event manager applet EIGRP_TRAP_nbr_up
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*up"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Up"
```

确认连结正确地传送这些并且检查您的SNMP监控工具-输出也许轻微有所不同，并且依靠使用的工具：

您能通过Wireshark捕获也查看这些SNMP陷阱：

> **Note**:它取决于Wireshark的版本，字符串不会在人类易读的文本，然而可以通过“snmp.value.octets被过滤包含“EIGRP”。



您能也验证连结发送这些在触发与Ethanalyzer的嵌入式活动管理器(EEM)。参见示例：

```
N7K-A-Admin# ethanalyzer local interface mgmt display-filter snmp limit-c 0

Capturing on mgmt0
2017-07-12 15:43:37.431067 10.122.140.96 -> 172.18.121.3 SNMP 278 snmpV2-trap 1.3.6.1.2.1.1.3.0
1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.1.9.10.134.1.2.3.1.2.1 1.3.6.1.4.1.9.10.134.1.2.3.1.6.1
1.3.6.1.4.1.
9.10.134.1.2.3.1.7.1 1.3.6.1.4.1.9.10.134.1.2.3.1.9.1 1.3.6.1.4.1.9.10.134.1.2.3.1.10.1
1.3.6.1.4.1.9.10.134.1.2.3.1.11.1
```

Note:前NX-OS 7.x不给出我们选项配置反之将允许您监控整个记录日志为EIGRP消息然后过滤的**snmp-server enable traps Syslog**。此功能在版本被添加了 ， 7.x和以后。